JOURNAL OF NUMBER THEORY **61**, 39–43 (1996)
ARTICLE NO. 0135

Sets of Prime Numbers Satisfying a Divisibility Condition

Paul Erdős

Mathematics Institute, Hungarian Academy of Science, Realtanoda u. 13–15, H-1053 Budapest, Hungary

and

Anthony B. Evans

Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435

Received May 4, 1995

We study sets P of k primes that satisfy the condition $\gcd(\prod A - \prod B, \prod P) = 1$ whenever A and B are disjoint non-empty subsets of P. It is known that such sets of primes exist for all positive integers k. It is of interest to know the asymptotic behavior of n_k, the smallest natural number that is the product of k such primes. In this paper we derive asymptotic bounds for n_k. © 1996 Academic Press, Inc.

THE RESULTS

For P a set of prime numbers and A and B subsets of P, let us use $A - B$ to denote the set $\{p: p \in A, p \notin B\}$, $\prod A$ to denote the product $\prod \{p: p \in A\}$, and similarly $\prod (A - B)$ to denote the product $\prod \{p \in A, p \notin B\}$. By convention $\prod \varnothing = 1$. We are interested in those sets of primes P that satisfy the following condition:

$$\gcd\left(\prod A - \prod B, \prod P\right) = 1,$$

for all disjoint, non-empty subsets A, B of P. (*)

As an example, if $P = \{3, 5, 7\}$, then each of the numbers $5 - 3 = 2$, $7 - 3 = 4$, $7 - 5 = 2$, $3 \times 5 - 7 = 8$, $3 \times 7 - 5 = 16$, and $5 \times 7 - 3 = 32$ is relatively prime to $\prod P = 3 \times 5 \times 7 = 105$, and so P satisfies (*). An easy

0022-314X/96 $18.00

observation to make is that every set of two primes satisfies (*). The existence question for such sets of primes was settled by Erdős and Evans in [1]: For all k there exists a set of k primes satisfying (*). This was used to obtain a simple proof of Lindner *et al.*'s result [2] that any finite graph can be represented as an orthogonal Latin square graph.

We ask the following question: If P is a set of k primes satisfying (*), how small can $\prod P$ be? Let us set $n_k = \text{Min}\{\prod P: P \text{ a set of } k \text{ primes satisfying } (*)\}$. Values of n_k for small k are given in Table I. The column headed $p_1, ..., p_k$ contains the set of k primes whose product is n_k.

The last column of Table I needs some explanation. We are interested in the asymptotic behavior of n_k, and this leads us to study the sequence $\{(\log_2 n_k)/k^2\}$. While we do not know if this sequence converges or not, we will show that it is bounded. The main result of this paper is that all the limit points of this sequence lie in the interval $[1, \log_2 3]$. This implies that n_k lies asymptotically between 2^{k^2} and 3^{k^2}.

Before we treat the asymptotic behavior of n_k, let us learn a little more about sets of primes satisfying (*). Given a set P of k primes satisfying (*) that cannot be extended to a larger set of primes satisfying (*), we will establish a relationship between k and $\text{Min}\{p: p \in P\}$.

LEMMA 1. *Let P be a set of primes satisfying (*) and let $p \in P$. If A and B are (not necessarily disjoint) non-empty subsets of $P - \{p\}$, $|A| \geqslant |B|$, and $\prod A \equiv \prod B$ modulo p, then B is a subset of A and $\prod (A - B) \equiv 1$ modulo p.*

Proof. Let A, B, P, and p satisfy the conditions of the lemma. As $|A| \geqslant |B|$, $A - B = \varnothing$ if and only if $B = A$, in which case B is a subset of A and $\prod (A - B) \equiv 1$ modulo p. If $A - B \neq \varnothing$ and $B - A \neq \varnothing$ also, then $\prod (A - B) \equiv \prod (B - A)$ modulo p, as $\prod A = \prod (A - B) \prod (A \cap B)$, $\prod B = \prod (B - A) \prod (A \cap B)$, and $\prod (A \cap B) \not\equiv 0$ modulo p. But then $\gcd(\prod (A - B) - \prod (B - A), \prod P) \geqslant p$, which, as $A - B$ and $B - A$ are disjoint and non-empty, implies that P does not satisfy (*). Thus $B - A = \varnothing$ and so B must be a subset of A. But then $\prod A = \prod (A - B) \prod B \equiv \prod B$ modulo p, and $\prod B \not\equiv 0$ modulo p, and so $\prod (A - B) \equiv 1$ modulo p. ∎

TABLE I

k	$p_1, ..., p_k$	n_k	$(\log_2 n_k)/k^2$
2	2, 3	6	0.64624
3	3, 5, 7	105	0.74603
4	7, 11, 13, 23	23,023	0.90567
5	13, 17, 29, 41, 61	16,028,909	0.95737

LEMMA 2. *Let* $P=\{p_1, ..., p_k\}$ *be a set of* k *primes satisfying* (*). *We can extend* P *to a set of* $k+1$ *primes satisfying* (*) *if and only if, for* $i=1, ..., k$, *there exists an integer* n_i *satisfying the following conditions*:

(a) n_i *is not divisible by* p_i

(b) $(n_i \prod B)-\prod A$ *is not divisible by* p_i *for any pair* A, B *of disjoint subsets of* $P-\{p_i\}$, A *non-empty*, B *not necessarily non-empty*.

Proof. If there exists a prime $q \notin P$ such that $P \cup \{q\}$ satisfies (*), then $n_i = q$, for all i, will satisfy conditions (a) and (b).

Suppose, for $i=1, ..., k$, there exists an integer n_i satisfying conditions (a) and (b). Let a be congruent to n_i mod p_i for $i=1, ..., k$. The existence of such an a is guaranteed by the Chinese remainder theorem. Let q be a prime in the sequence $\{(p_1 \cdots p_k)\, n+a\}$. It is routine to verify that $P \cup \{q\}$ will satisfy (*) if and only if q does not divide $\prod A - \prod B$, whenever A and B are non-empty disjoint subsets of P. This condition rules out only finitely many values for q, whereas, by Dirichlet's theorem, there are an infinite number of primes in the sequence $\{(p_1 \cdots p_k)\, n+a\}$. Hence there exists a prime q for which $P \cup \{q\}$ satisfies (*). ∎

Applying Lemmas 1 and 2 yields a simple sufficient, but not necessary, condition for a set of primes satisfying (*) to be extendible to a larger set of primes satisfying (*).

COROLLARY 1. *Let* P *be a set of primes satisfying* (*). *If* $\prod A \not\equiv 1$ *modulo* p, *for all* $p \in P$ *and any non-empty subset* A *of* P, *then* P *can be extended to a larger set of primes satisfying* (*).

Proof. Pick $n_i = 1$ for all i. ∎

THEOREM 1. *If* P *is a set of* k *primes*, $k \geqslant 2$, *satisfying* (*), *and* $p = \text{Min}\{q: q \in P\}$, *then* $k \leqslant \log_2(p-1)+2$.

Further, if P *cannot be extended to a set of* $k+1$ *primes satisfying* (*) *then* $k \geqslant \text{Min}\{r: 3^{r-1}-2^{r-1} \geqslant p-1\} =$ *one of* $\lceil \log_3(p-1) \rceil + 1$ *or* $\lceil \log_3(p-1) \rceil + 2$.

Proof. Let S be the set of non-empty subsets of $P-\{p\}$. If $A, B \in S$, $A \neq B$, $|A| \geqslant |B|$, and $\prod A \equiv \prod B \equiv 1$ modulo p, then, by Lemma 1, $\gcd(\prod (A-B) - \prod B, \prod P) \geqslant p$, violating (*). Hence $\prod A \equiv 1$ modulo p for at most one element A of S, and if $\prod A \not\equiv 1$ modulo p, $A \in S$, then there is at most one other element B of S for which $\prod A \equiv \prod B$ modulo p. Thus $2^{k-1}-1 \leqslant 1+2(p-2)$, from which it follows that $k \leqslant \log_2(p-1)+2$.

It follows from Lemma 2 that P can always be extended to a larger set of primes satisfying (*) if for each $q \in P$ there is an integer n_q, not divisible

by q, for which $n_q \not\equiv \prod A / \prod B$ modulo q for any pair A, B of disjoint subsets of $P - \{q\}$, A non-empty, B not necessarily non-empty. But the number of ordered pairs (A, B) of disjoint subsets of $P - \{q\}$, A non-empty, B not necessarily non-empty, is $3^{k-1} - 2^{k-1}$. Hence, if P cannot be extended to a larger set of primes satisfying (*) then $3^{k-1} - 2^{k-1} \geqslant q - 1 \geqslant p - 1$, from which it follows that $k \geqslant \text{Min}\{r: 3^{r-1} - 2^{r-1} \geqslant p - 1\}$.

It is an exercise to show that $\text{Min}\{r: 3^{r-1} - 2^{r-1} \geqslant p - 1\}$ must equal one of $\lceil \log_3(p-1) \rceil + 1$ or $\lceil \log_3(p-1) \rceil + 2$. ∎

As an example, if P is a set of k primes satisfying (*), the smallest of which is 5, then $k \leqslant 4$, and if P cannot be extended to a larger set of primes satisfying (*) then $k = 3$ or 4. Both of these possibilities occur as $\{5, 7, 13\}$ and $\{5, 7, 11, 149\}$ are both sets of primes that satisfy (*) and neither of these sets can be extended to a larger set of primes satisfying (*).

Now we consider the asymptotic behavior of the sequence of numbers n_k.

THEOREM 2. (a) *For $k \geqslant 2$, $(\log_2 n_k)/k^2 > 1 - 2/k$.*

(b) *For $\varepsilon > 0$, $(\log_2 n_k)/k^2 < \log_2(3 + \varepsilon)$ for all k sufficiently large.*

Proof. (a) Let P be a set of k primes satisfying (*), $k \geqslant 2$, and let $p = \text{Min}\{q: q \in P\}$. By Theorem 1, $p \geqslant 2^{k-2} + 1$ and hence $n_k > (2^{k-2} + 1)^k > 2^{k^2 - 2k}$. Thus $(\log_2 n_k)/k^2 > 1 - 2/k$.

(b) Let $x = (3 + \varepsilon)^k$ and let I be the interval $(x/2, x)$. By the prime number theorem, the number of primes in the interval I is $\beta(x)\, x/\log x$, where $\beta(x) \to 1/2$ as $x \to \infty$.

Let P be a set of m primes in I satisfying (*). How large can m be? Given a prime q in I, the set $P \cup \{q\}$ will satisfy (*) unless one of the following occurs:

(i) $q \in P$.

(ii) q divides $\prod A - \prod B$, for some pair of non-empty disjoint subsets A and B of P.

(iii) p divides $(q \prod A) - \prod B$ for some $p \in P$ and some pair A, B of disjoint subsets of $P - \{p\}$, B non-empty.

How many of the primes $q \in I$ are thus eliminated? Condition (i) eliminates precisely m of these primes. Let A and B be disjoint non-empty subsets of P. Now $\prod A - \prod B < x^{m-1} < 2^{m-1} q^{m-1} < q^{2m}$, for all $q \in I$. Thus fewer than $2m$ of the primes in I can divide $\prod A - \prod B$. Further, counting $\prod A - \prod B$ and $\prod B - \prod A$ the same, there are fewer than $(3^m)/2$ differences $\prod A - \prod B$ of products. Thus condition (ii) eliminates fewer than $3^m m$ of the primes in I. For a given choice of $p \in P$, and A and B subsets of $P - \{p\}$, at most one of the primes $q \in I$ can be a solution to

$q \prod A - \prod B \equiv 0$ modulo p, as should $q < q'$, $q \in I$ both be solutions; then $q \equiv q'$ modulo p and, for some positive integer n, $q' = q + np > x$, and so $q' \notin I$. Now, for any $p \in P$, there are fewer than 3^m possible choices for A and B, disjoint subsets of $P - \{p\}$, B non-empty. Hence, condition (iii) eliminates fewer than $3^m m$ of the primes $q \in I$. Thus the number of the primes $q \in I$ eliminated is at most $m + 2(3^m m)$.

Thus any set P of m primes in I satisfying (*) can be extended to a larger set of primes in I satisfying (*) if $m + 2(3^m m) < \beta(x)\, x/\log x$. More particularly, there exists a set of k primes in I satisfying (*) if $k + 2(3^k k) < \beta(x)\, x/\log x$. But for k sufficiently large $k + 2(3^k k) < (3+\varepsilon/2)^k < \beta(x)\, x/\log x$ as $x = (3+\varepsilon)^k$. Thus, for k sufficiently large, $n_k < x^k = ((3+\varepsilon)^k)^k$ and $\log_2 n_k/k^2 < \log_2(3+\varepsilon)$. ∎

Thus the sequence $\{\log_2 n_k/k^2\}$ is bounded and all its limit points lie in the interval $[1, \log_2 3]$. We pose the following question: Does $\lim_{n \to \infty}[(\log_2 n_k)/k^2]$ exist? If the answer is yes, then $n_k = \alpha^{(1+o(1))\,k^2}$ as $k \to \infty$, for some α, $2 \leqslant \alpha \leqslant 3$. If this is the case, what is α?

ACKNOWLEDGMENT

We thank Carl Pomerance for his helpful suggestions.

REFERENCES

1. P. Erdős and A. B. Evans, Representations of graphs and orthogonal latin square graphs, *J. Graph Theory* **13**, No. 5 (1989), 593–595.
2. C. C. Lindner, E. Mendelsohn, N. S. Mendelsohn, and B. Wolk, Orthogonal latin square graphs, *J. Graph Theory* **3** (1979), 325–338.